Amendments to the Claims

This listing of the claims as amended will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A method, comprising:

executing [[an]] a first authentication protocol, wherein a terminal authentication protocol comprises

authenticating an identity of a network entity by the terminal in a communication system;

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data, from the terminal to the network entity; and

determining, based on the terminal authentication data, whether to provide the terminal with access to a service,

wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

2. (Previously Presented) A method as claimed in claim 1, further comprising:

forming the test data by applying the authentication function to the challenge data at an authentication functionality; and

sending the test data from the authentication functionality to the network entity,

wherein the determining comprises forming network authentication data by applying the predetermined function to the test data and the key at the network entity, and

wherein the determining further comprises providing the terminal with access to the service only when the terminal authentication data equals the network authentication data.

3. (Previously Presented) A method as claimed in claim 1, further comprising:

sending the key from the network entity to the authentication functionality;

forming the test data by applying the authentication function to the challenge data at the authentication functionality; and

forming network authentication data by applying the predetermined function to the test data and the key at the authentication functionality.

4. (Previously Presented) A method as claimed in claim 3, further comprising:

sending the terminal authentication data from the network entity to the authentication functionality; and

sending, from the authentication functionality to the network entity, an indication of whether the terminal authentication data equals the network authentication data,

wherein the determining comprises providing the terminal with access to the service only when the indication is that the terminal authentication data equals the network authentication data.

5. (Previously Presented) A method as claimed in claim 3, further comprising:

sending the network authentication data from the authentication functionality to the network entity,

wherein the determining comprises providing the terminal with access to the service only when the indication is that the terminal authentication data equals the network authentication data.

6. (Previously Presented) A method as claimed in claim 1, wherein the terminal authentication data is formed as a cryptographic checksum.

7. (Previously Presented) A method as claimed in claim 1, wherein the network entity is co-located with the authentication functionality.

8. (Previously Presented) A method as claimed in claim 1, wherein an identity module of the terminal is configured to perform the authentication function.

9. (Original) A method as claimed in claim 8, wherein the identity module is user-removable from the terminal.

10. (Previously Presented) A method as claimed in claim 8, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

11-12. (Cancelled)

13. (Previously Presented) A method as claimed in claim 8, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

14. (Previously Presented) A method as claimed in claim 1, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning

protocol, a protected extensible authentication protocol, or an extensible authentication protocol-tunneled transport layer security.

15. (Previously Presented) A method as claimed in claim 1, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

16. (Previously Presented) A method as claimed in claim 1, wherein the said message is a dedicated authentication message.

17. (Previously Presented) A method as claimed in claim 1, wherein the predetermined function is used for derivation of a session key to be used for one of encryption or authentication of communications between the terminal and the network entity.

18. (Previously Presented) A system, comprising:

a terminal configured to apply authentication functions to input data to form response data; and

a network entity configured to provide access to a service,

wherein the system is configured to perform an authentication method of executing an authentication protocol, wherein the authentication protocol comprises

authenticating an identity of the network entity by the terminal in the system;

sharing a key between the terminal and the network entity for use in

securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity; and

determining, based on the terminal authentication data, whether to provide the terminal with access to a service;

wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

19. (Previously Presented) A system as claimed in claim 18, wherein the system is further configured to execute a linking protocol by forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol, and forming at the

network entity secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol,

wherein the secret session keys are configured to secure the subsequent communications between the terminal and some network element.

20. (Previously Presented) A method as claimed in claim 1, further comprising:

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol; and

forming at the network entity secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol,

wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

21-22. (Cancelled)

23. (Previously Presented) A method as claimed in claim 1, further comprising:

executing a third authentication protocol for authentication of the terminal comprising:

sharing between an authentication functionality and the challenge data;

forming response data and another key at the terminal by applying the authentication function to the challenge data;

sending the response data to the authentication functionality from the terminal;

authenticating the terminal at the authentication functionality using the response data; and

applying the authentication function to the challenge data to duplicate the another key.

24. (Previously Presented) A method as claimed in claim 23, wherein the third authentication protocol is an authentication and key agreement protocol or any protocol of the extensible authentication protocol family.

25. (Previously Presented) A method as claimed in claim 24, wherein the test data comprises one or both of an authentication and key agreement protocol integrity key value or an authentication and key agreement protocol cipher key value.

26. (Previously Presented) A method, comprising:

executing an authentication protocol, wherein the authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system, and

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network

entity; and

executing another authentication protocol comprising

receiving challenge data from the network entity at the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity; and

receiving access to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

27. (Previously Presented) A method as claimed in claim 26, wherein the terminal authentication data is formed as a cryptographic checksum.

28. (Previously Presented) A method as claimed in claim 26, wherein the network entity is co-located with an authentication functionality.

29. (Previously Presented) A method as claimed in claim 26, wherein an identity module of the terminal is configured to perform the authentication function.

30. (Previously Presented) A method as claimed in claim 29, wherein the identity module is user-removable from the terminal.

31. (Previously Presented) A method as claimed in claim 29, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

32. (Previously Presented) A method as claimed in claim 29, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

33. (Previously Presented) A method as claimed in claim 26, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

34. (Previously Presented) A method as claimed in claim 26, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

35. (Previously Presented) A method as claimed in claim 26, wherein the message is a dedicated authentication message.

36. (Previously Presented) A method, comprising:

executing an authentication protocol, wherein the authentication

protocol comprises

sending an identity of a network entity for authentication by a terminal in a communication system;

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sending challenge data from the network entity to the terminal for forming test data at the terminal by applying an authentication function to the challenge data;

receiving a message comprising terminal authentication data from the terminal at the network entity;

determining, based on the terminal authentication data, whether to provide the terminal with access to a service;

providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

37. (Previously Presented) A method as claimed in claim 36, wherein the terminal authentication data is formed as a cryptographic checksum.

38. (Previously Presented) A method as claimed in claim 36, wherein the network entity is co-located with an authentication functionality.

39. (Previously Presented) A method as claimed in claim 36, wherein an identity module of the terminal is configured to perform the authentication function.

40. (Previously Presented) A method as claimed in claim 39, wherein the identity module is user-removable from the terminal.

41. (Previously Presented) A method as claimed in claim 39, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

42. (Previously Presented) A method as claimed in claim 39, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

43. (Previously Presented) A method as claimed in claim 36, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

44. (Previously Presented) A method as claimed in claim 36, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

45. (Previously Presented) A method as claimed in claim 36, wherein the message is a dedicated authentication message.

46. (Previously Presented) A method as claimed in claim 36, wherein the predetermined function is used for derivation of a session key to be used for one of encryption or authentication of the subsequent communications between the terminal and the network entity.

47. (Previously Presented) An apparatus, comprising:

a processor configured to apply an authentication function to input data to form response data, and to execute an authentication protocol,

wherein the authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system, and

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity;

wherein the processor is further configured to execute another authentication protocol comprising

receiving challenge data from the network entity at the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity;

receiving access to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

48. (Previously Presented) An apparatus as claimed in claim 47, wherein the terminal authentication data is formed as a cryptographic checksum.

49. (Previously Presented) An apparatus as claimed in claim 47, wherein the network entity is co-located with an authentication functionality.

50. (Previously Presented) An apparatus as claimed in claim 47, wherein an identity module of the terminal is configured to perform the authentication function.

51. (Previously Presented) An apparatus as claimed in claim 50, wherein the identity module is user-removable from the terminal.

52. (Previously Presented) An apparatus as claimed in claim 50, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

53. (Previously Presented) An apparatus as claimed in claim 50, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

54. (Previously Presented) An apparatus as claimed in claim 47, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

55. (Previously Presented) An apparatus as claimed in claim 47, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

56. (Previously Presented) An apparatus as claimed in claim 47, wherein the message is a dedicated authentication message.

57. (Previously Presented) An apparatus, comprising:

a processor configured to execute an authentication protocol, wherein the authentication protocol comprises

sending an identity of a network entity for authentication by a terminal in a communication system; and

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity;

wherein the processor is further configured to execute another authentication protocol comprising

sending challenge data from the network entity to the terminal for forming test data at the terminal by applying an authentication function to the challenge data;

receiving a message comprising terminal authentication data, from the terminal at the network entity;

determining, based on the terminal authentication data, whether to provide the terminal with access to a service;

providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

58. (Previously Presented) An apparatus as claimed in claim 57, wherein the terminal authentication data is formed as a cryptographic checksum.

59. (Previously Presented) An apparatus as claimed in claim 57, wherein the network entity is co-located with an authentication functionality.

60. (Previously Presented) An apparatus as claimed in claim 57, wherein an identity module of the terminal is configured to perform the authentication function.

61. (Previously Presented) An apparatus as claimed in claim 60, wherein the identity module is user-removable from the terminal.

62. (Previously Presented) An apparatus as claimed in claim 60, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

63. (Previously Presented) An apparatus as claimed in claim 60, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

64. (Previously Presented) An apparatus as claimed in claim 57, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

65. (Previously Presented) An apparatus as claimed in claim 57, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

66. (Previously Presented) An apparatus as claimed in claim 57, wherein the message is a dedicated authentication message.

67. (Previously Presented) A computer program product embodied on a computer readable storage medium, the computer program product being configured to control a processor to perform a method comprising:

executing an authentication protocol, wherein the terminal authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system;

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data, from the terminal to the network entity; and

determining, based on the terminal authentication data, whether to provide the terminal with access to a service,

wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

68. (Previously Presented) A computer program product embodied on a computer readable storage medium, the computer program product being configured to control a processor to perform a process comprising:

executing an authentication protocol, wherein the authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system, and

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

receiving challenge data from the network entity at the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity;

receiving access to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the session key; and

forming a secret key by at least applying a predetermined function to the test data using the session key, the session key binding the authentication protocol and the another authentication protocol.

69. (Previously Presented) A computer program product embodied on a computer readable storage medium, the computer program product being configured to control a processor to perform a method comprising:

executing an authentication protocol, wherein the authentication protocol comprises

sending an identity of a network entity for authentication by a terminal in a communication system;

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sending challenge data from the network entity to the terminal for forming test data at the terminal by applying an authentication function to the challenge data;

receiving a message comprising terminal authentication data from the terminal at the network entity;

determining, based on the terminal authentication data, whether to

provide the terminal with access to a service;

providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key; and

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the first authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.